

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>6</sup> : <b>G06F 12/14</b>		A1	(11) International Publication Number: <b>WO 97/04394</b>
			(43) International Publication Date: 6 February 1997 (06.02.97)
(21) International Application Number: PCT/AU96/00440			(81) Designated States: JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  Published With international search report.
(22) International Filing Date: 12 July 1996 (12.07.96)			
(30) Priority Data: PN 4186 14 July 1995 (14.07.95) AU PN 9866 15 May 1996 (15.05.96) AU			
(71)(72) Applicant and Inventor: DRAKE, Christopher, Nathan [AU/AU]; G.P.O. Box 343, Sydney, NSW 2001 (AU).			
(54) Title: COMPUTER SOFTWARE AUTHENTICATION, PROTECTION, AND SECURITY SYSTEM			
(57) Abstract			
<p>A software-based computer security enhancing process and graphical software-authenticity method, and a method to apply aspects of the two are disclosed. The process provides protection against certain attacks on executable software by persons or other software used on the computer. Software using this process is protected against eavesdropping (the monitoring of software, applications, the operating system, disks, keyboard, or other devices to record (steal) identification, authentication or sensitive data such as passwords, User-ID's, credit-card number and expiry dates, bank account and PIN numbers, smart-card data, biometric information (for example: the data comprising a retina or fingerprint scan), or encryption keys), local and remote tampering (altering software to remove, disable, or compromise security features of the altered software) examination (viewing the executable program, usually with the intent of devising security attacks upon it), tracing (observing the operating of an executable program step-by-step), and spoofing (substituting counterfeit software to emulate the interface of authentic software in order to subvert security) by rogues (e.g.: Trojan Horses, Hackers, Viruses, Terminate-and-stay-resident programs, co-resident software, multi-threaded operating system processes, Worms, Spoof programs, key-press password captures, macro recorders, sniffers, and other software or subversions). Aspects include executable encryption, obfuscation, anti-tracing, anti-tamper and self-verification, runtime self-monitoring, and audiovisual authentication (math, encryption, and graphics based method permitting users to immediately recognise the authenticity and integrity of software). The figure in the specification depicts the many components and their interaction.</p>			
<p>The diagram illustrates a computer system architecture. A User (23) is shown interacting with a central processing unit (41). The system includes several components: 51 (a dashed box representing a secure environment), 31 (a component within the secure environment), 52 (a component within the secure environment), 17 (a component outside the secure environment), 18 (a component outside the secure environment), and 50 (a component outside the secure environment). Arrows indicate the flow of data and control between these components.</p>			

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

## COMPUTER SOFTWARE AUTHENTICATION, PROTECTION, AND SECURITY SYSTEM

BACKGROUND OF THE INVENTION

5       The present invention relates to a computer program having enhanced security features, and also to a system and method for enhancing the security features of a computer program. In particular, the present invention relates to such a program, and the system and method for creating the program, having increased security features to prevent ID-Data (as defined hereafter) eavesdropping and/or theft and/or to ensure authenticity.

10

DESCRIPTION OF THE PRIOR ART

Computers are becoming widely interconnected and heavily relied upon to process and store sensitive information. The risk of unauthorised access to computers and information has increased with this increased interconnectivity.

15       Many security advances exist in the areas of identification & authentication of users, cryptography, virus prevention, and the like, however - almost all of these advances ultimately rely upon computer software. Most computer systems are, or are accessed by, small personal computers, and most software used on these personal computers is susceptible to "local attacks" - attacks which are mounted from inside said personal computers against said software by other software or people.

20       Passwords, User-ID's, credit-card numbers and expiry dates, bank account and PIN numbers, smart-card data, biometric information (for example: the data comprising a retina or fingerprint scan), cryptographic keys, and the like are all examples of identification, authentication or similar data which is either sensitive in itself, or may allow access to sensitive, restricted or other information or services. Hereafter, the term ID-Data will be used to refer to the abovementioned identification, authentication  
25       or similar data, excluding ID-Data which is valid only for a single use, or which is designed to expire at regular intervals of less than two minutes.

Illegal access to computer system information can be obtained by exploiting various security flaws found in computer software products. A common flaw is the susceptibility of said software to the theft of ID-Data either directly from said software as it executes, or from the operating system or  
30       hardware on which said software is executing. Another common flaw is the susceptibility of said software to illegal modification. Such modifications may remove, disable, or compromise the security features of said software.

Viruses, Terminate-and-stay-resident programs (TSRs), co-resident software, multi-threaded operating system processes, Trojan Horses, Worms, Hackers, Spoof programs, key-press password  
35       capturers, macro-recorders, sniffers, and the like can be effective at stealing ID-Data and are examples of (a) rogue software or (b) people capable of subverting security software or (c) software

which can be configured for illegitimate purposes. Hereafter, the term rogue software will be used to refer to software or subversions such as the abovementioned (a) (b) and (c), used for the purpose of stealing ID-Data. The definition of our term "rogue software" when used herein also includes software or other means used to tamper with other software. The term tampering is defined hereafter.

- 5        There are many ways to introduce rogue software into a computer system. Viruses spread automatically by introducing themselves. Trojan-Horses are usually introduced by tricking users into allowing them to execute (such as by masquerading as a new or well-known computer game or other product). Existing security problems may be utilised to introduce rogue software; some well known problems include Java bugs, errors, or oversights, ineffective physical security (for example:
- 10        permitting rogue software to be introduced directly on floppy disk by an intruder), electronic mail attachments which automatically execute or execute after a simple mouse-click, incorrect security settings on internet, world-wide-web, TCP/IP or modems, and tampering (see definition hereafter) with legitimate software in-transit as it flows from remote internet sites into a users computer, to name a few.
- 15        Rogue software, once introduced, can steal ID-Data as mentioned hereinbefore. It may monitor keyboard (for example: by recording every key, as the user presses each one, in order to steal a password as it is being typed in), serial-port, mouse, screen, or other devices to steal ID-Data directly from them. It may monitor other software, applications, the operating system, or disks to steal ID-Data from there also. Once stolen, this ID-Data may be stored locally (for example: in memory or on-
- 20        disk) or transmitted to remote locations (for example: by modem or network) or used immediately to perform illegal operations. Hereafter, the term eavesdropping will be used to refer to the monitoring of a computer to record ID-Data.

- For example, a key press recorder could secretly, and unbeknown to the computer user, record all the keys pressed by the user into a hidden systems file. The information recorded could include a
- 25        user's password and other sensitive information which an organisation would obviously wish to protect.

- Additionally, rogue software may remove, disable, or compromise existing computer software security features by modifying the memory, disk, or other image of said computer software. Rogue software may also utilise tampering techniques to alter existing computer software in order to steal ID-
- 30        Data from it, or may attach itself to existing computer software (as is the case with many computer viruses). Hereafter, the term tampering will be used to refer to the abovementioned modification of computer software. Tampering may take place either locally (within a users PC) or remotely (for example: at one of the points which a computer program passes through as it is being download).

- Further, counterfeit software can be substituted for legitimate software. The counterfeit will
- 35        appear real to a computer user, but actually acts to subvert security, such as by stealing ID-Data. Sometimes called "Spoof" programs or Trojan Horses, counterfeit software of this type may invoke the original legitimate software after having stolen ID-Data, so as not to arouse a users suspicion.

Another potential security flaw found in computer software products is susceptibility to examination and reverse-engineering. Known (but generally secret) and other security problems or

mistakes can be discovered by hackers and the like from the examination of existing computer software and by tracing its operation.

Additionally, Computer software piracy is a growing problem, and the existing simple means which prevent this problem (such as registration or serial numbers and customer-names being encoded  
5 within the product) are becoming less effective.

There is necessity within the try-before-you-buy software market for vendors to employ effective features which allow old software to expire without fear of hackers or the like removing said expiry features and for secure registration of software to be provided through the use of software unlock-codes.

10 There is also need for software to be able to prevent security attacks upon itself (ie: tampering) and upon its own attack-detection code. There may also be a future need for software to identify the attacker for subsequent prosecution.

There also exists cases where untamperable software usage metering may be desirable, and where effective password-protection of software execution may also be desirable.

15 Known advances in certain areas of computer security have been successful and documented. There have been some advances in anti-virus technology which help detect and prevent certain security problems. There have been numerous advances in hardware-assisted computer security add-ons and devices, such as smartcards and biometric input devices. There have been advances in cryptographic techniques. Generally, all of these advances require authentic, un-tampered-with computer software in  
20 order to work. There have been relatively few advances in software-based integrity self-checking (eg: tamper protection), and no prior software-based advances in preventing eavesdropping or the electronic theft of ID-Data, and no prior software-based advances in self-authentication.

#### SUMMARY OF THE INVENTION

25 This invention describes a process which substantially enhances the security of computer software (hereafter referred to as the improved process) and a method by which to apply said improved process (hereafter referred to as the applicator).

The improved process consists of including computer code to automatically detect tampering of said computer software, and computer code to prevent the theft of ID-Data by replacing existing  
30 vulnerable (to rogue software eavesdropping or attack) software or operating system code with secure equivalents which utilise anti-spy techniques (as described later in this document).

Preferably, the improved process also consists of including computer code to prevent de-compilation, reverse-engineering, and disassembly by the inclusion of obfuscating code inserts, and the use of executable encryption.

35 Preferably, the improved process also consists of including code to prevent execution-tracing

and debugging by the use of code designed to detect and prevent these operations.

Preferably, the improved process consists of, or also includes, human-recognisable audio-visual components which permit the authenticity of said computer software to be easily verified by the user on each invocation using techniques described later in this document.

- 5           The idea which lead to the creation of this invention can be summarised as follows:- If a piece of computer software that is executing can be shown to be the genuine article, and this software can protect itself against eavesdropping, and this software can prevent tampering of itself, then is it possible for this software to function in a secure manner, even within an insecure operating system. This invention permits the creation of such a piece of computer software - having a tangible, useful  
10 security advantage and hence improving its value.

#### BRIEF DESCRIPTION OF THE DRAWINGS

- Fig.1 illustrates the standard operation of a computer system known in the prior art;  
Fig.2 illustrates the known operation of a rogue or "spoof" program;  
15 Fig.3 illustrates application code updated with the preferred embodiment;  
Fig.4 illustrates the known operation of a rogue eavesdropping program;  
Fig.5 illustrates the interaction of the components of the updated application;  
Fig.6 illustrates the general structure of the preferred embodiment of the applicator;  
Fig.7 illustrates a standard layout for a program to be executed on a computer system;  
20 Fig.8 illustrates the standard layout of an EXE header under the MS-DOS operating system.  
Fig.9 illustrates a standard layout of an EXE program under MS-DOS;  
Fig.10 illustrates an altered executable form constructed in accordance with the specific embodiment;  
Fig.11 illustrates a first stage of execution of the new.exe executable;  
Fig.12 illustrates a second stage of execution of the new.exe executable file;  
25 Fig.13 illustrates a third stage of execution of the new.exe executable file.

#### DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

- As will be described hereinafter, the present invention has general applicability to many different operating systems including Microsoft DOS (Trade Mark), Apple Macintosh Operating  
30 System, Unix (Trade Mark) etc.

- Described hereafter are several security-enhancing techniques to combat eavesdropping. Security is provided by (a) hampering examination of software-code or operating system code or parts thereof through the use of the encryption or partial encryption of said code, (b) preventing the disassembly of said code through the inclusion of dummy instructions and prefixes and additional code  
35 to mislead and hamper disassembly (ie: obfuscating inserts), (c) preventing the computerised tracing of the execution of said code (for example: with code debugging tools) through the use of instructions to detect, mislead, and hamper tracing, (d) preventing tampering of said code through the use of scanning to locate alterations, either or both on-disk and in memory either once at the start of execution, or continuously upon certain events, r (e) preventing ID-Data theft through the inclusion of secure

input/output routines (for example: routines to bypass the standard operating system keyboard calls and use custom-written higher-security routines as a replacement) to replace insecure computer-system routines. Hereafter, the term anti-spy will be used to refer to any combination of one or more of the abovementioned techniques [(a) through (e) or parts thereof] used to prevent eavesdropping.

- 5 Referring now to Fig.1 there is illustrated the standard scenario for "running" a given executable program 16, under the control of a computer operating system 17 on a computer 18. In the preferred embodiment of the present invention, the executable program 16 is subjected to modification, as will be described hereinafter, to ensure its integrity and improve its security.

- 10 There are five aspects of this inventions improved process, although said process is still substantially improved even if not all of them are present. These aspects are: (1) Preventing eavesdropping (2) preventing disassembly and examination (3) detecting tampering (4) preventing execution-tracing and (5) ensuring authenticity.

The preferred embodiment of these aspects of the present invention will now be described.

**Aspect 1. Preventing eavesdropping.**

- 15 As hereinbefore described, it is desirable to prevent rogue software from eavesdropping on ID-Data. By replacing software which is vulnerable to eavesdropping with equivalent software which is far more secure, this purpose is achieved. To remove the vulnerability from said equivalent software, replacement routines may communicate directly with the hardware of the computer (for example, they may communicate with the keyboard circuitry instead of using the system-supplied (and hence  
20 possibly insecure) application interface keyboard-entry function-calls.) while disabling system interrupts which would permit rogue software to eavesdrop. Said replacement routines are coded to store ID-Data retrieved in a secure manner. ID-Data is not stored in full in plaintext (ie: unencrypted) in system or application buffers.

**Aspect 2 Preventing disassembly and examination.**

- 25 As hereinbefore described, it is desirable to hamper disassembly (or de-compilation or reverse engineering) to protect software against eavesdropping and tampering, and to hinder examination of said software which might lead to secret security problems or mistakes being disclosed.

- Obfuscating inserts can successfully prevent automatic disassembly. Obfuscation is achieved by following unconditional jump instructions (for example, Intel JMP or CLC/JNC combination or  
30 CALL (without a return expected) or any flow-of-control altering instruction which is known not to return to the usual place) with one or more dummy op-code bytes which will cause subsequent op-codes to be erroneously disassembled (for example, the Intel 0xEA prefix will cause disassembly of the subsequent 4 op-codes to be incorrect, displaying them as the offset to the JMP instruction indicated by the 0xEA prefix instead of the instructions they actually represent).

- 35 Dummy instructions may also be included to hamper disassembly by deliberately misleading a disassembler into believing a particular flow of control will occur, when in fact it will not.

Flow of control can be designed to occur based upon CPU flag values determined from instructions executed a long time ago. Together with tracing prevention, this makes manual disassembly nearly impossible.

- 5 The majority of the executable portions of the software can be encrypted for external storage. The decryption taking place in-memory after the software is loaded from external sources, under the control of a decryption "header" which prevents its own tampering and disassembly etc. This makes manual and automatic disassembly nearly impossible, since the decryption should be designed to fail if tampering or tracing is detected.

### Aspect 3 Detecting tampering.

- 10 As hereinbefore described, it is desirable to detect tampering, since this may lead to the reduction of software security.

- 15 This can be achieved with the use of code which is protected from disassembly and examination through obfuscation and encryption, which re-reads its own external-image and compares it with its known memory image or precalculated check-data to detect hot-patching (ie: the modification of software sometime after it has been loaded from disk, but (usually) before execution of the modified section has commenced).

Additionally, the software can scan the memory image of itself one or more times, or continuously, to ensure that unexpected alterations do not occur.

- 20 Certain modifications to the external copy of software are reflected in subtle changes to the environment in which the modified software will be executed (for example: the size of the code, if altered, will be reflected in the initial code-size value supplied to the executing program being incorrect.). Additionally, certain modification to the operating system and environment of said software can also be monitored (for example: certain interrupt vector table pointers in Intel-processor applications) to detect unexpected changes by rogue software. These changes can also be detected to prevent tampering.

- 25 Once tampering is detected, program flow-of-control needs to be changed so that the potential compromise associated with ID-Data theft is avoided. This may be the security-enhanced program terminating with a message indicating that its integrity has been compromised before all of the ID-Data is entered. Alternatively, the fact that tampering has been detected may be kept secret and the ID-Data retrieved, however, immediately upon retrieval, the ID-Data entered can be invalidated thus preventing access to that which the now potentially compromised ID-Data would have otherwise allowed. This latter method allows for the possibility of security-enhanced software informing remote or other authorities that tampering was detected and possibly other information, such as what specifically was altered and by whom. Care must be taken to ensure the integrity of the "remote-informing" code before ID-Data entry is permitted.

35 It will be apparent to one skilled in the art of low-level software programming that the five aspects described herein may be combined to provide substantially stronger security than any aspect



taken on its own. For instance, to combine tamper-detection with encryption, the precalculated check-data as derived during tamper-detection described hereinbefore may actually be one part of the decryption-key which is required to successfully decrypt the remaining executable software. If prevention-of-tracing and environment characteristics (including debugger detection as described hereafter) are additional portions of said decryption-key, it makes the determination of said decryption-key by any person or computer program other than the secure original an extremely difficult, if not impossible, task.

Further, it will also be apparent to one skilled in the art of low-level software programming that a simple construct such as a JNE to alter program flow-of-control after tampering has been detected is insufficient, since the JNE construct itself is subject to tampering. The denryption process described hereinbefore is preferable since there is no single point of alteration that can possibly yield a tampered executable that would execute. Indeed, the executable protected with encryption will not even be transformed into its intended form if tampering is detected.

#### Aspect 4 Preventing execution-tracing.

Apart from "spoofing" (described in aspect 5 hereafter) the last resort of a rogue who is prevented from disassembly, tampering, and eavesdropping on software is to trace the execution of said software in order to facilitate the compromise of its security. Hampering tracing (tracing is sometimes called debugging) prevents this.

There are numerous methods of detecting a debug-environment (ie: when tracing is taking place). When combined with decryption and tamper-protection as hereinbefore described, it makes the rogues task of detecting and bypassing debug-detection extremely difficult. Reference and examples to Intel and MS-DOS environments follow hereafter, although it will be apparent to one skilled in the art that these and similar methods are applicable on other platforms.

Standard Intel x86 interrupts 1 and 3 are used by debuggers to facilitate code tracing. By utilising these interrupts (which are not normally used by normal applications) in security-enhanced software, it hampers debugging, since built-in debugging functions are now not automatically available.

Monitoring the system timer to determine if software execution has spent too long accomplishing certain tasks can detect a situation where code tracing has been in effect and a breakpoint was reached.

Disabling the keyboard will hamper debuggers, since tracing instructions are usually issued from the keyboard. Similarly, disabling other places from where tracing instructions are usually issued (eg: serial ports, printer ports, and mouse) or displayed (eg: screen) will also hamper tracing.

System interrupts can be re-vectored for use within the secure software to perform tasks not usually performed by those interrupts. Debuggers usually rely upon system interrupts also, so to do this would usually disable or destroy a debugger being used to trace the software.

Disabling interrupts and performing timing-sensitive instructions between them will further hamper debugging. When tracing software, instructions are usually executed one-at-a-time in order for the user to understand their operation. Many system interrupts must occur regularly (eg: timer and memory re-fresh operations), so debuggers usually do not disable interrupts even when they encounter  
5 an interrupt-disabling instruction. If timers and the like are re-vectored in two separate stages, any timer (etc) interrupt occurring inbetween the two stages will fail, and usually crash the computer. Further, interrupts can be disabled or enabled using obscure means (with flag-altering instructions for example) to hamper tracing.

Discretely testing the status of disabled or enabled system facilities (eg: interrupts, keyboard, vector-pointers) to ensure that a debug-environment has not altered or by-passed them will seriously  
10 hamper tracing also.

Certain computer processors have instruction caches. In some circumstances, it is possible to alter the instructions immediately before the CPU encounters them, but the altered instruction will not be executed normally because the cache copy has the "old" one still. In debug environments, the cache  
15 is usually flushed, so any altered instructions will actually be executed. This again hampers tracing.

Using strong cryptographic schemes, such as DES, or RSA or the like will prevent the examination of any decryption routines from revealing a simple patch to disable said routines.

When tracing software, the program stack is usually used by the debugger either during the tracing operations or at other times. This is easily detected, and by using the area of the stack which  
20 will be destroyed by unexpected stack-use for code or critical data, software can be designed to self-destruct in this situation.

Scanning the command environment and the execution instruction can detect the execution of software by unusual means. Searching for "DEBUG" in the command line, or scanning memory for known debuggers for example will detect tracing. Additionally, by detecting which operating system  
25 process initiated the load of the software, unexpected processes (eg: debuggers) can be detected.

Monitoring system buffers (eg: the keyboard memory buffer) or hardware (eg: the keyboard circuitry and internal buffers) for unexpected use (eg: keyboard input and processing is occurring when the software is not requesting it) will also detect debuggers, which usually rely in part on system functions in order to operate.

Building a process or multiple processes which are traditionally difficult to trace, such as a resident or child process which executes during system interrupts or after the parent process has terminated will again hamper tracing.

Bypassing system routines (eg: in DOS, using direct memory writes instead of DOS system calls to revector interrupts) will further hamper debugging and rogue software monitoring, as will  
35 unravelling loop constructs (which will make tracing long and cumbersome).

Code checksums and operating-system checks (eg: interrupt table pointers) can be designed to detect debug-breakpoint instruction inserts or other modifications. Using the result of the checksum

for some obscure purpose (eg: decryption, or (much later) contr 1-flow changes) will further hamper tracing.

5 It will be apparent to one skilled in the art of low-level software programming that a combination of techniques to detect, prevent, and mislead tracing will provide a mechanism making tracing very difficult, if not impossible. At the very least, it will require an expert with very expensive tools and perhaps some understanding of the original software design a very long time to make any debugging progress - a situation which is recognised in military software security accreditation worldwide as highly desirable.

**Aspect 5 Ensuring authenticity.**

10 In accordance with an aspect of the present invention there is provided a method of providing for a secure entry of ID-Data in a computer system comprising activating a visual display or animation and/or audio feedback (hereinafter called an audio/visual component) as part of said secure entry of ID-Data so as to hamper emulation of said secure entry process.

Preferably, the animation includes feedback portions as part of the ID-Data entry process.

15 Preferably, the animation is repeatable and varied in accordance with the information entered. The animation preferably comprises 2.5D or 3D animation and includes animation of any ID-Data input.

Preferably, the animation is designed to tax the computer resources utilised and thereby making any forgery thereof more difficult.

20 Notwithstanding any other forms which may fall within the scope of the present invention, preferred forms of the invention will now be described, by way of example only, with reference to the accompanying drawings.

25 In the preferred embodiment of the present invention the user interface for the acquiring of ID-Data is secured whereby the duplication of the interface is rendered mathematically complex such that cipher-code breaking techniques are required to produce a counterfeit look-alike interface. By making the authentication interface (ie: ID-Data entry screen - for example: a logon screen or a screen for entering credit card details) unable to be emulated, tampered with, or reversed engineered, the application program allows for a higher degree of security and authenticity even in insecure environments such as the Internet or home software applications.

30 Referring now to Fig.2, there is illustrated a classic form of rogue attack on a computer system. In this form of rogue attack, a rogue's "spoof" program 22 is inserted between application software 16 and the user 23. The application 16 normally has a portion 24 devoted to ID-Data entry and verification or the entry of commercially sensitive information (including passwords etc) to the application in addition to the application code 25. The spoof program 22 is designed to exactly reflect  
35 the presented user interface of ID-Data entry code 24 to the user. The user 23 is then fooled into utilising the masquerading spoof program 22 as if it was the application 16. Hence the user can be tricked into divulging secret information to the spoof program 22. An example may include a classic

"login spoof" wherein the spoof program 22 prints the login prompt (ie: ID-Data entry) message on the screen and the user mistakes the login prompt for a legitimate one, supplying a user name and password to this program 22 which records this information as well as passing it on to the login code 24 of application 16 so as not to arouse the suspicion of user 23 - or by issuing a message, such as

5 "incorrect password, please try again" and then passing control to the login code 24 of application 16.

Referring now to Fig.4, there is illustrated a relatively new form of rogue attack 40. This form of attack proceeds similarly to the spoof attack of Fig.2, with the following difference. Instead of a spoof program 22, a rogue program 41 is inserted which secretly eavesdrops on ID-Data entry code 24, or on application code 25, or on operating system 17, or on hardware 18 or elsewhere in order to

10 steal sensitive information directly from the legitimate application. Since the legitimate application is still actually executing, the users suspicion is not aroused, since rogue program 41 is generally invisible to the user 23. Alternatively, executable program 16 may have been tampered with (as hereinbefore described) to reduce its security, alleviating the necessity for the presence of rogue program 41.

15 In Fig.5, there is illustrated in detail the structure of an application 50 constructed in accordance with the preferred embodiment running on computer hardware 18. Fig.5 is similar to Fig.4 with the important difference that user 23 now communicates directly with secure drivers 51 which are part of the secure ID-Data entry program code 31 which is utilised by the security-enhanced (eg: tamper protected) application code 52. It can be seen that the user 23 no longer communicates

20 with the operating system 17 or the unprotected computer hardware 18, thus the rogue program 41 can no longer eavesdrop on ID-Data.

In Fig.3, there is illustrated, in more general terms than Fig.5, the structure of an application 30 constructed in accordance with the preferred embodiment wherein secure ID-Data entry program code 31 is provided which is extremely difficult to replicate, eavesdrop upon or subvert. The secured ID-

25 Data entry program code 31 can be created, utilising a number of different techniques.

Firstly, the executable portion of the secured ID-Data entry code can be protected against tracing, disassembly, tampering, viewing, reverse engineering, keyboard entry theft, eavesdropping, hot patching and other attacks by transforming the secured ID-Data entry program code 31 from its normal executable form 16 (Fig.2) to a corresponding secured form of executable (as hereinbefore

30 described - refer aspects 1 to 4). These techniques are preferably applied to the application code 16 in general or less preferably specifically limited to the ID-Data entry portions 24 thereof.

Additionally, the secure ID-Data entry program code 31 is itself created. This code 31 preferably comprises a complex graphical user interface series of screens and animation designed to make duplication by a rogue thereof extremely difficult.

35 Initially, the complex user interface should include facilities to disable any frame buffer recording devices, the disablement occurring before each frame is displayed. Also, where a multi-tasking operating system is in use, or where context switching is enabled, switching out of the interface screen is preferably disabled or ID-Data entry procedures encrypted or terminated when the interface screen is swapped out. The images presented which form part of the ID-Data entry screens

comprise complex 3D animation sequences having a high degree of complexity and extensive use of screen colours and screen resolution in addition to visual design so as to make copying thereof extremely difficult.

The complex computer graphics can be created utilising standard techniques. For information on how to create complex 3D imagery, reference is made to "Computer Graphics, Principles and Practice" by Foley, Van Dam et al, published 1990 by Addison-Wesley Publishing Company or other standard textbooks on generation of computer graphics. Reference is also made to the numerous internet news groups and archives on graphics and games programming, specifically to: comp.graphics.research, comp.graphics.rendering, comp.graphics.raytracing, comp.graphics.misc, comp.graphics.digest, comp.graphics.animation, comp.graphics.algorithms, comp.graphics, alt.graphics.pixutils, alt.graphics, rec.games.programmer, comp.sys.programmer, comp.sys.ibm.programmer, comp.sys.ibm.pc.programmer, comp.os.msdos.programmer, comp.msos.programmer, alt.msos.programmer. Reference is also made to "PC Games Programmers Frequently Asked Questions" document available on the internet, via rec.games.programmer and elsewhere.

By encoding a complex 3D image which forms part of the ID-Data entry screens, the hurdle requirement of a rogue to reverse engineer the complex imagery is substantially increased. The inclusion of graphical animation is advantageous in preventing static screen shot duplication attacks by a rogue form succeeding.

As noted above, it is preferable that traditionally difficult graphical programming techniques are employed wherever possible, with the aim of making it more detectable for a user interacting with the system to discern lesser copies of the animation. Suitable 3D animation can include the introduction of shadows, the lighting of pseudo-3D animated objects, transparent or translucent objects, shiny, reflective, or mirrored objects, gravitational effects in animated objects, single-image-random-dot-stereogram bitmaps or backdrops, translucent threads, effects, such as diffraction patterns, screen masks, backdrops, colour palette "animation", complex animated objects resistant to simple hidden-surface removal techniques known to those skilled in the art and directed to hindering duplication.

Further, the animation can take into account:

1. Thwarting attempts at compression of the ID-Data entry screens. This can be achieved by having animation which has low visual entropy and having many graphical elements which are altered from frame to frame in a manner which is highly discernible to the human viewer. Apart from being difficult to replicate, complex 3D computer imagery having low entropy or redundancy will require large amounts of storage space for a rogue attempt at duplication based on recording the screen output and therefore be more readily discernible to the user should this form of attack be mounted.

2. The animation is further preferably designed to thwart a successful replay attack which is based on providing only a subset (limited number of frames) of the screen animation to a viewer. This can be achieved, for example, by the inclusion of several animated spheres which "bounce" around the screen and change colours in a manner that is recognisable to the viewing user but which is not readily repeatable. A replay of only a subset of the screen animations to the viewer will be highly evident in

this case when, upon looping, the user is alerted to a problem when the animation "skips" or "jumps" and does not operate in a previously smooth manner. This makes it difficult for a rogue spoof program to copy the animation without including all parts of it.

3. Most importantly, the graphics presented can be customised to the input data entered. For example, the information entered by a user can be rendered and/or animated by the secure ID-Data entry program code 31 (Fig.3). As an example, in an ID-Data entry program, when a user types in their user name, the animation can be created letter by letter. For example, when typing in the user name "CHRIS" each letter could be rendered differently depending on those characters previously typed. For example, the letter "I" might appear as a large "barbers-pole" which spirals and changes colour, speed, size, and/or position and is slightly transparent, thereby allowing the animated seen which is a backdrop to the character to be discerned through the character itself. For example, in the above example, the letter "I" would only appear as the specific animated barbers pole that is does if the previous letters entered were "C", "H", and "R" respectively.

The utilisation of a unique sequence of animation based on a user's input of information sensitive data increases the difficulty of creating any "spoof program" attack on the application 30. This is especially the case since the executable code of application 30 is preferably in an encrypted form. The use of animation being particular to the order in which characters are entered is particularly advantageous as the computational complexity of replication is substantially increased.

A similarly effective animation technique is to produce only one graphical object after entry of each portion of ID-Data, such as a computer-generated human's face, but have the features of said face be determined by a hash or cryptographic function based upon the users input. For example, after entry of the ID-Data "CHRIS" (in this example, the individual characters may not, themselves, be based on the abovementioned generation procedure), a teenage girl's face with long blonde hair and blue eyes may be displayed. If the "S" was instead a "D", the face would be entirely different. The ID-Data used for producing an object for display should not be ID-Data which is designed not to appear on-screen when entered (eg: a password), since the display of a corresponding object would give a rogue information on which to base guesses of the secret ID-Data.

By utilising cryptography or having complex formulas to determine the sequencing of animation, the rogue programming the corresponding spoof program shall have to crack the cryptographic scheme in order to get the selection of character animation correct for any generalised attack. In the abovementioned example, a rogue will have to determine the algorithm for producing the face, since human beings are adept at recognising faces, and will immediately notice if the face displayed on the screen is incorrect. Such a technique allows for a mathematically secure, visual method to guarantee the authenticity of the software which generates the screen feedback. The user of the software is instructed to note their own particular animation sequence and to immediately discontinuing utilisation of the application 30 should that sequence ever change. The user may also be instructed to contact a trusted person, such as the supplier or operator of the application to confirm that the animation sequence they witness is the authentic sequence intended by said supplier.

Further, the particular animation presented for a particular application 30 can be further

customised for each application so as to be distinct (such as by the incorporation of the applications name as part of the animated image).

5 Further hindrance for a rogue programmer can be created by hand coding portions of the animation in assembly language so as to generate the maximum possible complexity and interaction in the animation with the highest level of detail for individual workstation computers. This further raises a hurdle allowing for the easier detection of rogue spoof programs 22 which will often be written in a more convenient, higher level language (such as C or C++) which will also operate at a different speed, the user being instructed to look for speed differences.

10 Further, animated scene timing can be utilised, providing anti-looping and frame removal detection is still catered for. The animated scene timing allows for a user to detect unexpected irregularities in a frequently presented animated interface. By including in the animation some deliberate regularity (such as the rhythmic convergence of some parts of the animation in one particular spot), a rogue programming a spoof program shall also have to duplicate the preferably complex timing events necessary to accomplish this convergence. The regular nature of the scene  
15 timing should be high enough so that the user expects to see certain events and thereby making it difficult for a rogue spoof program to copy the animation without including all parts of it.

Preferably, where possible, all ID-Data is immediately encrypted which makes recovery of the ID-Data by a rogue through analysis of the computer program memory difficult. Preferably, public-key cryptographic methods (eg: Elliptic-curve, RSA or Diffie-Hellman cryptography) should be used  
20 making it impossible to reverse engineer the cryptographic code to decrypt any sensitive information should it be stolen in its encrypted form. Prohibiting all or most interrupts when data is to be entered and encrypting or hashing the sensitive information immediately so that it is only stored partially, or in an encrypted form, before re-enabling interrupts is one example of achieving this objective.

25 As a further alternative, analysis of a user's personal characteristics can be included as part of the interface. This can include attempts at recognition of a user's typing style (duration of keypresses, delays between subsequent keys, choice of redundant keys, mouse usage characteristics, etc) or by additional authentication techniques, including smartcards, biometric inputs such as finger prints detectors etc.

30 Further, the graphical animation routines can be "watermarked" by the secure ID-Data entry program code in that "hidden" information may be incorporated into the scene (for example "salted-checksums") to allow careful analysis of the output of secure ID-Data entry program code 31 to distinguish between original graphics animation and counterfeit animation. For example, the hidden information may be encoded in the least-significant bit of pixel data at selected locations of the animation.

35 The user determinable sequence of animation can also extend to the provided audio animation. For example, audio and other feedback techniques including music and speaking tones can be played in response to particular key stroke combinations. By utilising different voices and/or tones and/or volumes and pitches for each keystroke or combination, the security of the application 30 can, once again, be substantially increased. The change in voice intonation will be readily "learnt" by a user and

thereby further inhibit a rogue's ability to duplicate the same sequence of sounds or voices. Of course, the encoding of the voice system should be in an encrypted form.

Further, upon detecting any attempt to subvert the secure ID-Data entry program code 31 (eg: subsequent to detecting tampering), a notification message is preferably sent to a prosecuting body or the like where the application 30 is currently, or later becomes connected to a network such as the Internet, or by other means (eg: via Modem or by including coded information in public or other files).

For application programs 30 requiring activation by a host program executed on a different computer, a secure means of activation can be incorporated into the client application 30. The host and client intercommunication can issue challenge and response code authentication and verification utilising cryptographic systems such as public-key encryption and/or other standard means of overcoming data replay attacks and other threats designed to trick the secure client application 30 into activation.

It would be appreciated by a person skilled in the art that the process of coding any data entry process utilising these techniques, together with additional techniques to protect against recording, and eavesdropping, and executable protection techniques may be necessary to improve the security of the interface. Additionally, executable encryption, additional authentication, and other methods are desirable in producing the protected executable.

It would be appreciated by a person skilled in the art that numerous combinations, variations and/or modifications may be made to the present invention as described without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

#### Summary of the Applicator (of an improved process of security as hereinbefore described)

The preferred embodiment of the present inventions' method (hereinbefore described as the "applicator") by which to apply an improved process of security (as hereinbefore described) will now be described with reference to the accompanying drawings.

Referring now to Fig. 7, there is shown a standard format utilised for storing executables on disk, often occurring in the art, and in particular in conjunction with programs run on the above mentioned operating systems. The standard executable 16 normally comprises a header section 71, a code section 72, and a data section 73. The header section 71 normally stores a standard set of information required by the computer operating system 17 (Fig. 1) for running of the executable 16. This can include relocation data, code size etc. The code section 72 is normally provided for storing the "algorithmic" portion of the code. The data section 73 normally is utilised to store the data, such as constants, or overlays 92 utilised by the code section 72.

Turning now to Fig. 6, the preferred embodiment of an applicator program 60 is shown which takes as its input the executable program 16 and performs an obfuscating step 61, a ciphering step 62 and an anti-key press and authentication step 63 (described hereafter) which perform various transformations on the executable program 16 to produce a new executable program 30.



The obfuscating step 61 modifies the header 71 (Fig. 7) of the executable 16 in addition to inserting loading code which will be described hereinafter. The cipher step 62 encrypts the existing executable 16 and calculates check data (eg: a checksum) for the encrypted executable. The anti-key press and authentication step 63 replaces various insecure system calls with safe equivalent code and preferably inserts code to graphically represent the integrity of said executable program.

The newly formed executable 30 (new.exe) can be then stored on disk and the applicator program 60 completed, the new executable 30 replacing the old executable program 16.

When it is desired to run the replacement executable program 30, the replaced executable 30 (new.exe) executes the obfuscating code, previously inserted by applicator 60. The obfuscating code initially decrypts the executable program and validates the stored check-data before re-executing the decrypted executable.

The foregoing description of the preferred embodiment has been in general terms and it will be understood by those skilled in the art that the invention has general application to many different operating systems, including MS-DOS, Apple Macintosh OS, OS/2, Unix etc.

The most common operating system utilised today is the MS-DOS operating system. This operating system is designed to run on INTEL x86 microprocessors and includes a large number of historical "quirks" which give rise to greater complexity than would perhaps be otherwise required when designing a new operating system from "scratch". For illustrative purposes, there will now be presented a specific embodiment of the preferred embodiment designed to operate under the MS-DOS operating system. Unfortunately, the example is quite complex as it operates in the framework of the MS-DOS operating system. Therefore, it is assumed that the reader is familiar with systems programming under the MS-DOS operating system. For an extensive explanation of the inner workings of the MS-DOS operating system, reference is made to standard texts in this field. For example, reference is made to "PC Intern" by Michael Tischer, published in 1994 by Abacus, 5370 52nd Street, S.E. Grand Rapids, MI 49512. A second useful text in this matter is "PC Architecture and Assembly Language" by Barry Cauler, published 1993 by Carda Prints, 22 Regatta Drive, Edgewater, WA 6027, Australia.

The specific embodiment of the present invention will be described with reference to altering an "EXE" executable program under DOS in accordance with the principles of the present invention.

Referring now to Fig.9, there is shown the structure 90 of an executable ".EXE" program in MS-DOS as normally stored on disk. This structure is closely related to the structure 16 of Fig. 7 which illustrates the more general case. The structure 90 includes a header 71, otherwise known in MS-DOS terminology as the program segment prefix (PSP). This is normally followed by a relocation table 91 which contains a list of pointers to variables within a code area 72 which must be updated with an offset address when the program is loaded into a particular area of memory. The operation of the relocation table is well known to those skilled in the art of systems programming. The next portion of structure 90 is the code area 72 which contains the machine instructions for operation on the x86 microprocessor. This is followed by a program data area 73 which contains the data for code area 72. Finally, there may exist a number of overlays 92 which contain code which can be

utilised in a known manner.

Referring now to Fig.8, there is shown the structure of EXE file header 71 in more detail. The table of Fig.8 being reproduced from page 750 of the above mentioned Tischer reference. It should be noted that the header 71 includes a number of fields including, for example, a pointer 81 to the start of the code 72 (Fig. 7) and a pointer 82 to the relocation table 91 (Fig.9).

In the specific embodiment, the applicator program 60 (Fig. 6) proceeds by means of the following steps:

- (1) The executable program 16 is opened for reading and a determination made of its size.
- (2) The header 71 (Fig.9) of executable program 16 is then read in and a copy is stored within applicator program 60. A copy of the header 71 is written out to form part 101 of the new.exe file 30 as illustrated in Fig.10.
- (3) Next, from the fields 81, 82 of the header 71 (Fig. 8) a determination is made of the size of relocation table 91 of executable program 16.
- (4) Next, determination is made of the size of the executable code 72 and data portions 73.
- (5) The relocation table 91 is then read into the memory of the applicator program 60. As noted previously, the relocation table 91 consists of a series of the pointers to positions within code segment 72 which are required to be updated when loading the program.exe file into memory for execution. The relocation table is sorted 93 by address before being written out to the new.exe executable file at position 102.
- (6) As noted previously, the relocation table 91 consists of a series of pointers into code area 72. A determination is made of the size of a code, known as the "netsafe 1" code 104, the contents of this code will be described hereinafter. Next, a search is conducted of the sorted relocation table 102 to find an area between two consecutive pointers within code section 72 which is of greater magnitude than the size of netsafe 1 code 104. This area 94, designated part B in Fig.9 is located. If this code portioned 94 cannot be located the applicator program 60 exists with an error condition.

Upon finding code portion 94, the code portion 95, also denoted part A is encrypted and copied across to form new code portion 103. Code portion 94 is then encrypted and copied to an area 105 of new.exe 30. The netsafe 1 code 104 is then inserted by applicator 60. Code portion 96, also denoted part C is encrypted and copied across to form code portion 106. Data portion 73 and overlay portion 92 are copied into new.exe 30 as shown. A second portion of obfuscating code, denoted "netsafe 2" 107, the contents of which will be described hereinafter, is then inserted after overlays 92 and before code portion part B 105.

(7) The header 101 is then updated to reflect the altered layout of new.exe executable 30. Additionally, the initial address 109 of execution stored in header 101 is altered to be the start of netsafe 1 portion 104.

(8) As mentioned before, code portions 103, 106 and 105 are subjected to encryption or encipherment in accordance with step 62 of Fig.6. The encryption scheme utilised can be subjected to substantial variation. In this embodiment, the DES standard encryption scheme was utilised. This scheme relies on a fifty-six bit key for encryption and decryption and is well known in the art.

Once encrypted, it is necessary to store the decryption key in new.exe executable 30. A number of different methods can be utilised to store the key. The preferred method is to spread portions of the key to different positions within the executable 30. For example, bits of the key can be stored within the netsafe 1 code 104 and netsafe 2 code 107. Additionally, bits of the key can be stored within  
5 header portion 101. Also, it is envisaged that bits of the key can be stored in the condition codes which are a consequence of execution of various instructions within netsafe 1 area 104 and netsafe 2 area 107 and/or the operating system 17 (Fig.5), with the overall requirement being that the key can be later extracted using a predetermined algorithm.

(9) The next step is to patch the address of the start of code area 72 and netsafe 2 code area  
10 107 into the required locations within netsafe 1 area 104.

The netsafe 1 area is then written to the file containing new.exe executable 30.

(10) The area 106 is then encrypted as aforementioned and written to the executable 30 followed by overlays 92 and encrypted netsafe 2 code portion 107.

(11) As will become apparent hereinafter, upon execution of new.exe executable 30, netsafe 2  
15 area 107 is responsible for loading code portion 105 over the top of netsafe 1 area 104. Therefore, it is necessary to write the relevant addresses of the start and end of code portion 94 to the required position within netsafe 2 area 107.

(12) As will be described hereinafter, netsafe 2 area 107 is also responsible for decrypting the encrypted portions of codes 103, 104, 105, 106, and 107 and hence the netsafe 2 area 107 must also  
20 store this combined code size for later use on decryption.

Finally, a overall checksum for new.exe 30 is calculated and stored at the end of the file at position 108. This checksum is later used to verify the decryption procedures' success and to prevent the execution of "scrambled" code, which would be the result if new.exe 30 were tampered with.

As will be further described hereinafter, netsafe code areas 104 and 107 contain code to decrypt  
25 the encrypted areas of the new.exe 30, to repatch code portion 105 back to its original position, and to replace potentially insecure routines or easily spoofed screens normally utilised by the application (eg: unsafe keyboard drivers) with an alternative safe form of routine.

Upon execution of the new.exe executable 30, the executable starts at the start of netsafe 1, area 104 (Fig.11), as this address has been previously patched into position 109 (fig.10) of header 101  
30 (Fig.10). The netsafe 1 area 104 then performs the following steps (A1) to (A10):

(A1) The first step is to disable all the interrupts apart from those necessary for continued operation of the computer device 18 (Fig. 1) (for example, memory refresh cannot be disabled). The disabling of interrupts includes the disabling of the keyboard interrupt in order to stop amateur "code snoopers" from determining the operation of the code area 104.

(A2) The next step is to interrogate the calling environment of the operating system stack to  
35 ensure that the program new.exe was not called by a debugging program which is tracing the

operation of new.exe. Additionally, the data variables necessary for operation of netsafe 1 code area 104 are defined to be on the operating system stack (Refer Address 0EH and 10H in Fig.8). This stack will change unexpectedly when in a code snooping or debugging environment and will cause the debugger to crash, thereby stopping it from following the operation of new.exe executable 30.

5 (A4) The interrupt trap addresses are then altered in a two stage process. The first stage resets a first part of the SEG:OFF address format and occurs at this point with a second stage occurring at a later time as will be further described herein below. By staging the alteration of interrupt trap addresses, any code snooper will be further confused as said trap addresses will initially be garbage.

10 (A5) Any input from the keyboard is further disabled by informing the MS-DOS operating system to ignore any received keys.

(A6) The second stage of the revectoring of the normal debugging interrupts is then applied so that the normal debugging interrupts can be used by the decryption code, to be described hereinafter, thereby making debugging almost impossible.

15 (A7) A check is then made to ensure that the above processes have been successful in that the debugger interrupts do not point to any debuggers, the keyboard is still disabled and the operating system has disabled the acceptance of keys from the keyboard.

(A8) The key for decryption is then reconstructed utilising the reverse process to that utilised in storing the information located in the key.

20 (A9) Turning now to Fig. 11, there is shown the standard format of the executable new.exe 30 when executing in memory. As will be well known to those skilled in the art, an executing program under the MS-DOS system will include a stack 111 and work space 112. A memory allocation (Malloc) call is then done to set aside an area 113 for the loading in of the netsafe 2 code 107 of Fig.10. The disk copy of new.exe 30 (having the format shown in Fig.10) is then opened by the netsafe 1 code 115 and an encrypted copy of netsafe 2 code 107 (Fig.10) is then loaded in from the disk file, decrypted and stored in memory area 113. The relocatable pointers of the code contained within the netsafe 2 code 113 are then updated to reflect the position of the executable in memory.

(A10) Control is then passed to netsafe 2 code 113.

The code area netsafe 2, 113 then performs the following steps (B1) to (B4):

30 (B1) The portion of code of the disk copy denoted part B, 105 (Fig.10) is read in from disk in an encrypted format and written over the old netsafe 1 code 115.

(B2) As will be further described hereinafter, the netsafe 2 area 113 includes a number of keyboard routines which are preferably stored in an encrypted format. Therefore, the next step is to apply the decryption to any of the encrypted areas of netsafe 2 code area 113. After decryption, the netsafe 2 area 113 is checksummed and the result is tested against a prestored checksum to ensure the integrity of netsafe 2 area 113.

(B3) The disk copy of the new.exe is then again read in and checked against prestored check data to ensure that it has not been changed. Additionally, an attempt is made to read past the end of file of the disk copy of new.exe 30 (Fig.10) to ensure that no extension (eg: viral) has occurred.

5 (B4) The encrypted portions of the memory copy (Fig.11) of new.exe are then decrypted utilising the key and once decrypted, the decrypted portions are again checked and tested against predetermined data.

10 The next step in execution of the netsafe 2 code 113, is to replace insecure (eg: keyboard) system routines with a more secure method. Referring now to Fig.12, there is shown the current state of the new.exe executable in memory. The insertion of the more secure system routines then proceeds in accordance with the following steps (C1) to (C5):

(C1) Firstly, a second memory allocation is done to set aside an area 51 (Fig. 13) for the storing of the secure hardware routines (eg: keyboard). These routines are then copied from their area within netsafe 2 code 113 to the memory area 51.

15 (C2) Next, the ID-Data entry routines which are normally activated by the interrupt table 131 when dealing with ID-Data input are altered such that, rather than pointing to corresponding areas of the MS-DOS operating system 17, they point to the corresponding secure area 51. These interrupts include interrupt 9 which occurs when a key is pressed on a keyboard, interrupt 29h which reads a key and interrupt 16h which tests for the presence of a key.

20 (C3) The executable 30 (Fig.13) is then ready for execution and the registers are initialised, the memory area 113 deallocated & control passes to the original start address of executable program 16.

25 (C4) It will be evident, that when executing, all keyboard calls (or other ID-Data entry calls, if other than keyboard) will be passed to keyboard (or other) routines 51 with the keyboard hardware being interrogated directly by keyboard routines 51 to return information to the calling program. Keyboard routines 51 include a copy of the correct interrupt vector addresses for each keyboard routine and each time they are called, a check is made of the interrupt table to ensure that it has not been altered. Preferably, keyboard routines 51 protect the keyboard hardware by issuing controller reset or similar commands to flush the keyboard data out of the circuitry after said data is retrieved to prevent hardware eavesdropping, or routines 51 utilise the protected mechanisms of the central processor to protect said hardware from eavesdropping.

30 (C5) When the executable 30 terminates, interrupt 21h (an MS-DOS standard) is called. This interrupt is also revector to a corresponding area of routines 51. The termination code of keyboard routine area 51 restores the correct interrupt pointers in interrupt table 131 to point to the MS-DOS operating system 17, and clears the no-longer-needed program and data from memory before returning to the DOS operating system by calling the real interrupt 21.

35 The foregoing describes only one particular embodiment of the present invention, particularly to the operation of the MS-DOS operating system. It will be evident to those skilled in the art, that the principles outlined in the particular embodiment can be equally applied to other operating systems in

accordance with the objects of the present invention. Further, modifications, obvious to those skilled in the art, can be made thereto without departing from the scope of the invention.

#### **EXPLANATION AND PURPOSE OF CLAIMS**

5        Claims 1, 2, and 3 are independent. The invention in claim 1 covers any high security software protecting ID-Data by utilising anti-spy techniques, and tamper-protecting itself. Claim 2 is for a method of producing high security software, such as, but not limited to, that in claim 1. Claim 3 is for a new process of graphically representing the authenticity of high security software, such as, but not limited to, that in claim 1 or produced by claim. 2.

10        Claims 4, 5, 6, 7, 8, and 9 add preferred components to the high-security enforcing functions of the software in claim 1. Claim 10 adds a tracing-prevention preferred component to claim. 9

      Claims 11, 12, 13, 14, 15, 16, 50, and 53 add preferred components to the security-applicator method of claim 2.

15        Claims 17 to 49 inclusive and claims 51 & 52 outlines the specific area of protection that this invention affords a computer program acting as a user interface (eg: ID-Data entry screen). Specifically, they specifies how this invention applies in the areas of protecting an interface against counterfeiting (i.e.: hampering the possibility that a fake copy of said interface can be successfully presented to a user to fool said user into entering information into the fake interface), and protecting an interface against malicious (or otherwise) tampering, examination, emulation, and eavesdropping.

CLAIMS

1. A high security executable program comprising:
  - (a) purpose-written computer input routines within or accessed by software on a computer system for the entry of ID-Data (as hereinbefore defined), and
  - 5 (b) anti-spy techniques (as hereinbefore defined) within said input routines which prevent or hamper eavesdropping (as hereinbefore defined) on said ID-Data, and
  - (c) tamper-detection techniques (as hereinbefore defined) within or accessed by said software to detect tampering (as hereinbefore defined) and techniques which, upon detection of tampering, either disallow the subsequent entry of ID-Data into said input routines, or which invalidate said ID-Data in order to disallow current and subsequent access to that which said ID-Data would have otherwise allowed
- 10 2. A method of altering an original executable program to form an altered executable program having increased security, said method comprising the steps of:
  - (a) inserting obfuscating code into a first number of predetermined areas of said executable program; and
  - 15 (b) encrypting portions of said executable program for later decryption upon execution; such that, upon execution of said altered executable program, said execution includes the steps of:
  - (c) decrypting the altered executable program; and
  - (d) restoring said altered executable program to said original executable program.
- 20 3. A method of providing for a secure entry of input information in a computer system comprising:
  - (a) activating a visual display or animation and/or audio feedback (hereinafter called an audiovisual component) as part of said secure entry of input information so as to hamper emulation of said secure entry process; and
  - 25 (b) audio/visual component feedback of two or more of:
  - (c) all or part of said input information;
  - (d) all or part of information based upon some transformation of said input information;
  - (e) all or part of some transformation of all or part of the software comprising said audio/visual component and/or the computer operating system upon which said audio/visual component
  - 30 operates.
4. A method as claimed in claim 1 additionally including the replacement of code which is vulnerable to eavesdropping (as hereinbefore defined) with equivalent code which removes said vulnerability; said equivalent code which communicates directly with the hardware of the computer while disabling system interrupts or other functions which would permit rogue software (as
- 35 hereinbefore defined) to eavesdrop.
5. A method as claimed in claim 1 additionally including one or more automatic disassembly (as hereinbefore defined) techniques of (a) obfuscating inserts (as hereinbefore defined), (b) dummy instructions (as hereinbefore defined), or (c) executable encryption (as hereinbefore defined).
- 40 6. A method as claimed in claim 1 additionally including code to detect tampering (as hereinbefore defined) by re-reading its own external-image or its internal memory image and

comparing said image or a calculated check of said image with pre-calculated check-data or known identical equivalents.

7. A method as claimed in claim 1 additionally including code to automatically memory-scan the said software one or more times before or during execution of said software to detect  
5 tampering (as hereinbefore defined).

8. A method as claimed in claim 1 additionally including code to store or communicate details of detected tampering for later examination, said details including all or part of said tampered software, and/or other information available to said tampered software from said computer system.

9. A method as claimed in claim 1 additionally including code to prevent, or detect and  
10 subsequently prevent tracing, or mislead code debuggers and execution tracing by utilising debugger trap facilities for the normal operation of said security-enhanced software, and/or monitoring system timers or including timing-sensitive instructions or monitoring CPU stack contents or monitoring system buffers to detect the activity of code debuggers, and/or disabling facilities including the keyboard, serial ports, printer ports, mouse, screen or system interrupts in order to hamper code  
15 debuggers, and/or testing that the disabled status is still true of said facilities to detect code debuggers, and/or utilising system interrupts which would ordinarily be used by code debuggers for the custom purposes of said security-enhanced software, and/or utilising CPU instruction caches together with self-modifying code to mislead code debuggers, and/or scanning or interrogating the operating system or executable-load-process to detect code debugger instructions or environments.

20 10. A method as claimed in claim 9 additionally including a process or multiple processes which are resident or child processes of said security-enhanced software which execute during system interrupts or after the parent process has terminated in order to hamper tracing.

11. A method as claimed in claim 2 wherein said obfuscating code includes replacement  
25 codes for insecure system routines and said execution further includes the step of: (e) replacing the execution of said insecure system routines with said replacement codes.

12. A method as claimed in claim 2 wherein said steps (c) and (d) occur while simultaneously substantially disabling eavesdropping on the operation of said steps (c) and (d) by any rogue program.

30 13. A method as claimed in claim 2 wherein said step (a) includes inserting a portion of said obfuscating code into the code area of said original executable program.

14. A method as claimed in claim 11 wherein said step (e) includes altering portions of an interrupt vector table to point to said replacement codes.

35 15. A method as claimed in claim 2 wherein said step (b) includes the storing of a decryption key in a plurality of predetermined areas of said altered executable program.

16. A method as claimed in claim 15 wherein said predetermined areas include the condition codes of predetermined instructions of said altered executable program.



17. A method as claimed in claim 3 wherein said audiovisual component has repeatable characteristics during subsequent invocations of said entry process, such that said audiovisual component on each invocation of said entry process has a predetermined resemblance to the audiovisual component of all other invocations of said entry process.
- 5 18. A method as claimed in claim 3 wherein said audiovisual component is varied in accordance with the information entered.
19. A method as claimed in claim 3 wherein said audiovisual component comprises moving parts and/or includes 2.5-dimensional animation or 3-dimensional animation.
- 10 20. A method as claimed in claim 3 wherein said audiovisual component includes a representation of said input information.
21. A method as claimed in claim 20 wherein said input information representation comprises (a) display of a single graphical object and/or (b) production of a single audio-feedback sequence, after the entry of all or part of said input information.
- 15 22. A method as claimed in claim 20 wherein said input information representation includes animation of input characters and/or audible or other feedback determined by input characters.
23. A method as claimed in claim 22 wherein the representation of said input characters varies for each character based on the result of a predetermined transformation of the preceding input characters.
- 20 24. A method as claimed in claim 23 wherein said transformation utilises cryptographic or hashing methods.
25. A method as claimed in claim 3 wherein the ease by which faithful replication of said audiovisual component is substantially reduced by inclusion in said audiovisual component the techniques of on screen shadow rendering and/or spot or flood scene fighting effects and/or scene or object shading and/or transparent or translucent objects and/or shiny, reflective, or mirrored objects and/or real-time animation roughly obeying real world gravitational effects and/or single-image-random-dot-stereogram bitmaps or backdrops and/or partial scene masking effects and/or full or partial scene distortion or diffraction effects and/or animated objects designed to resist simple hidden-surface removal techniques and/or animated bitmaps and/or audible echo effects and/or differing audio voice effects and/or differing audio volume and/or differing audio tones or pitches.
- 30 26. A method as claimed in claim 3 wherein said audiovisual component is immediately recognisable to human beings and includes information which identifies to the user the application to which said audiovisual component belongs.
27. A method as claimed in claim 3 wherein the ease by which faithful replication of said audiovisual component is further reduced by inclusion in said audiovisual components animation object movement timing such that at near regular and frequent intervals regularities occur which are obviously recognisable to users of said entry process.
- 35 28. A method as claimed in claim 3 wherein said entry process including said audiovisual component utilises a substantial portion of the computational resources of said computer system.

29. A method as claimed in claim 3 wherein said entry process code responsible for said audiovisual component is coded in the assembly language of the computer system.

30. A method as claimed in claim 3 wherein recording said audiovisual component by said computer system is disabled.

5 31. A method as claimed in claim 3 wherein (a) the facility to suspend or swap-out said entry process is either disabled, or (b) immediately upon suspension request, said entry process is protected against subsequent examination by encryption or by termination and removal from memory of said entry process, or (c) where the facility to allow the central processor or processors of said computer system to execute code other than the code of, or the code necessary for said entry  
10 process is either disabled or else said entry process is protected against examination.

32. A method as claimed in claim 3 wherein said entry process hampers simple recording by utilising the maximum practicable use of audiovisual framerate, and/or audiovisual resolution, and/or screen colours, and/or audiovisual design in said audiovisual component on said computer system.

15 33. A method as claimed in claim 3 wherein said entry process hampers the compression of recorded output from said audiovisual component by utilising high audiovisual entropy and/or by the inclusion of random or other noise in said audiovisual component.

34. A method as claimed in claim 3 wherein said audiovisual component includes continuous output such that the looping of only a subset of said output shall not reproduce a copy  
20 largely indistinguishable to said audiovisual component.

35. A method as claimed in claim 1 or claim 3 wherein said ID-Data or said input information is encrypted with some cryptographic process or hashed immediately upon entry and a plain text equivalent is not stored by said computer system.

36. A method as claimed in claim 35 wherein disablement of one or more interrupt  
25 instructions (or equivalent CPU devices) is utilised to protect said cryptographic or said hash process of said ID-Data to hamper the recovery of said ID-Data by processes other than said entry process.

37. A method as claimed in claim 1 or claim 3 wherein said input routines or said secure entry process prevents the re-vectoring of system interrupts in order to protect said ID-Data or said  
30 input information from being stolen, by means of re-applying interrupt vector pointers one or more times and/or by means of examining interrupt assignments in order to perform a predetermined function should the expected assignments be altered.

38. A method as claimed in claim 1 or claim 3 wherein in order to further authenticate and/or identify said user, additional aspects of said ID-Data or said input information are used  
35 including the duration of individual key presses and/or mouse button presses and/or the delay between subsequent individual key presses or mouse button presses and/or the user's selection of particular keys when more than one equivalent exists and/or the acceleration or velocity characteristics of mouse usage and/or where said input information includes information from other sources including biometric and/or smartcard information.

39. A method as claimed in claim 1 or claim 3 wherein said input routines or said secure entry process authenticates itself using (a) executable code checksums of RAM or other images of its own executable code and/or data, (b) and/or comparison of memory with other stored copies of said executable code, (c) and/or decryption of said entry process (d) and/or detection of executable tampering by examination of the executable's environment (e) and/or comparison of executable size with expected values (f) and/or by attempting to read past the end of the executable file to determine that the size is correct; parts (a) through (f) occurring either upon initial load or during or after execution one or more times or continually during execution.

40. A method as claimed in claim 1 or claim 3 wherein said input routines or said secure entry process makes use of system interrupts to monitor itself in order to detect alteration of itself.

41. A method as claimed in claim 39 or claim 40 wherein said input routines or said secure entry process incorporates means by which to notify and/or transmit authentication failure details to a third person or process should said self authentication fail.

42. A method as claimed in claim 1 or claim 3 wherein said input routines or said secure entry process records a log of the usage and/or details of the user of said input routines or said secure entry process.

43. A method as claimed in claim 1 or claim 3 wherein said input routines or said secure entry process incorporates warnings within the executable image indicating that examination and/or tampering is prohibited.

44. A method as claimed in claim 3 wherein said audiovisual component contains watermark information incorporated into the scene to allow close inspection of said audiovisual component to distinguish between the genuine process and a close replica.

45. A method as claimed in claim 1 or claim 3 wherein said input routines or said secure entry process's loading and/or decryption routines are stored within the executable image in such a way as they initially replace other entry process routines and upon successful decryption and/or authentication, said other entry process routines are replaced.

46. A method as claimed in claim 1 or claim 3 wherein said input routines or said secure entry process hampers executable-code tracing through control-flow changes in debug environments or through disabling one or more system interrupts and/or disabling the keyboard and/or disabling the mouse or other input devices and/or making use of the program stack pointer to discern existence of a debug environment and/or utilising debug interrupts for program code operation and/or self-modification of executable code and/or examination of CPU flag registers and/or verification of disabled interrupts still-disabled state and/or verification of disabled keyboards still-disabled state and/or loading additional executable code into memory during execution.

47. A method as claimed in claim 1 or claim 3 wherein the executable image of said input routines or said secure entry process includes obfuscating assembly language dummy operation codes or instruction prefixes inserted after one or more unconditional branches to hamper executable disassembly and/or decompilation and/or reverse engineering.

- 26 -

48. A method as claimed in claim 1 or claim 3 wherein said input routines or said secure entry process is securely activated by its activation process and/or a host or server computer using a challenge/response activation protocol or using public or private key cryptographic methods.

5 49. A method as claimed in claim 1 or claim 3 wherein said input routines or said secure entry process is stored outside of said computer system memory in encrypted form and/or where said entry process employs techniques to hinder executable-code tracing and/or executable-code disassembly or disclosure or decompilation and/or executable-code tampering and/or executable-code hot-patching and/or reverse-engineering and/or pre, in, or post-execution executable-code recording, copying, eavesdropping or retrieval and/or theft of said input information from keyboard  
10 hardware or software or drivers.

50. A method as claimed in claim 2, 11, 12, 13, 14, 15, or 16 further comprising the insertion of one or more components as claimed in claims 1, 4, 5, 6, 7, 8, 9, 10, or 51.

51. A process as claimed in claim 3, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29,  
15 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, or 49 further comprising protecting all or part of said input routines or said secure entry process with zero or more components as claimed in claims 1, 4, 5, 6, 7, 8, 9, 10, or 0.

52. A method for providing for the secure input of information into a computer system, or  
20 A high security executable, substantially as hereinbefore described with reference to the accompanying drawings.

53. A method of altering an original executable program to form an altered executable program having increased security, substantially as hereinbefore described with reference to the accompanying drawings.

25

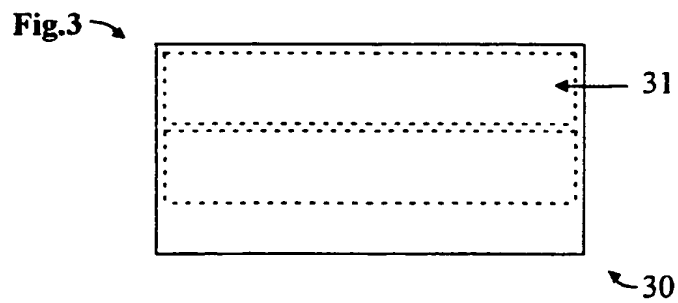
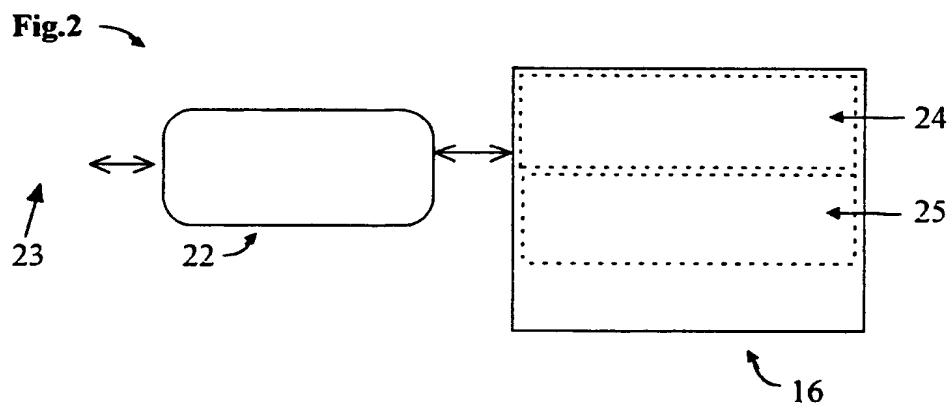
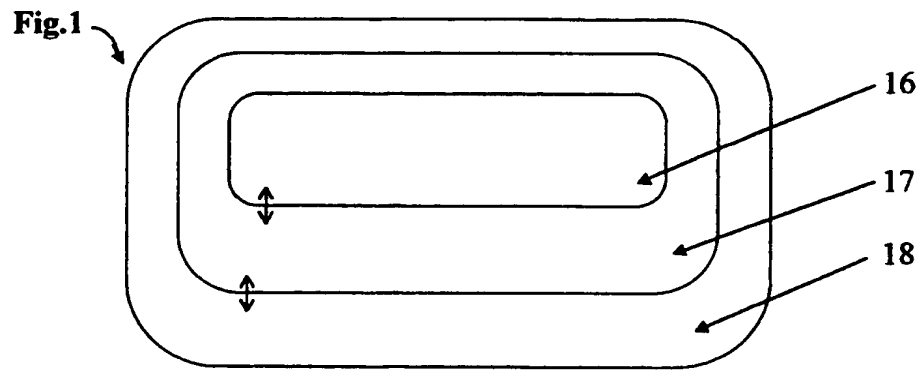


Fig.4

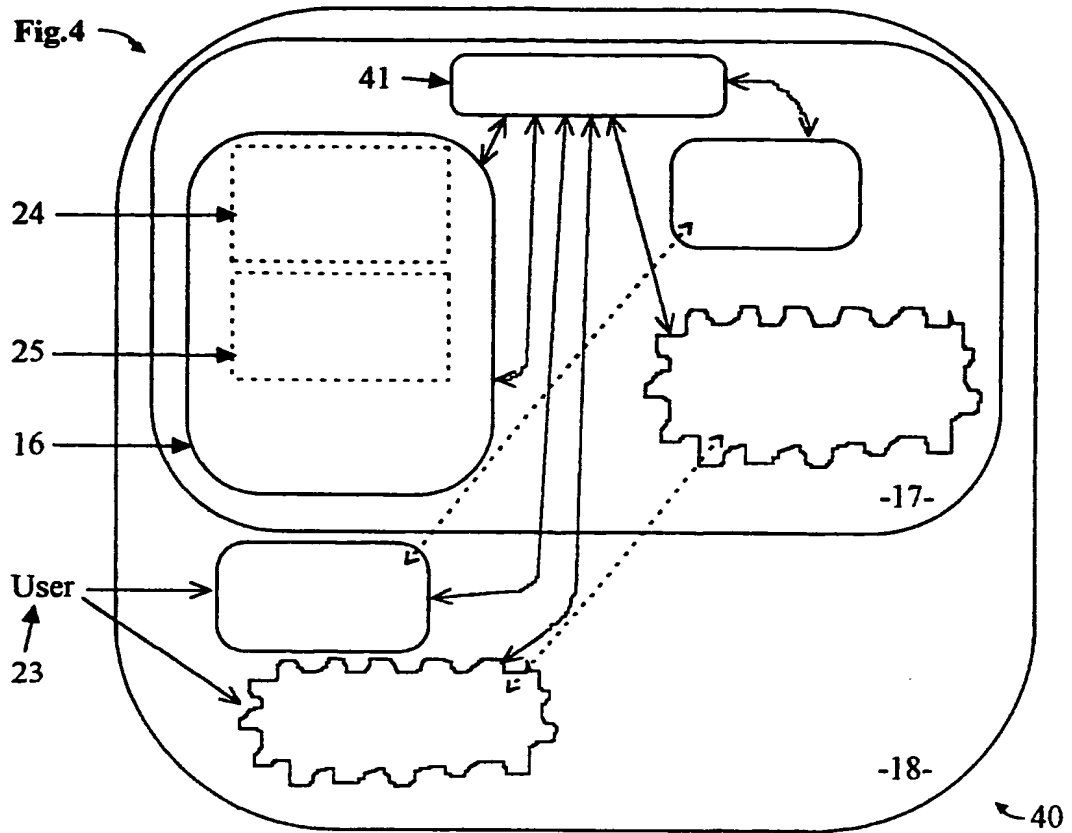
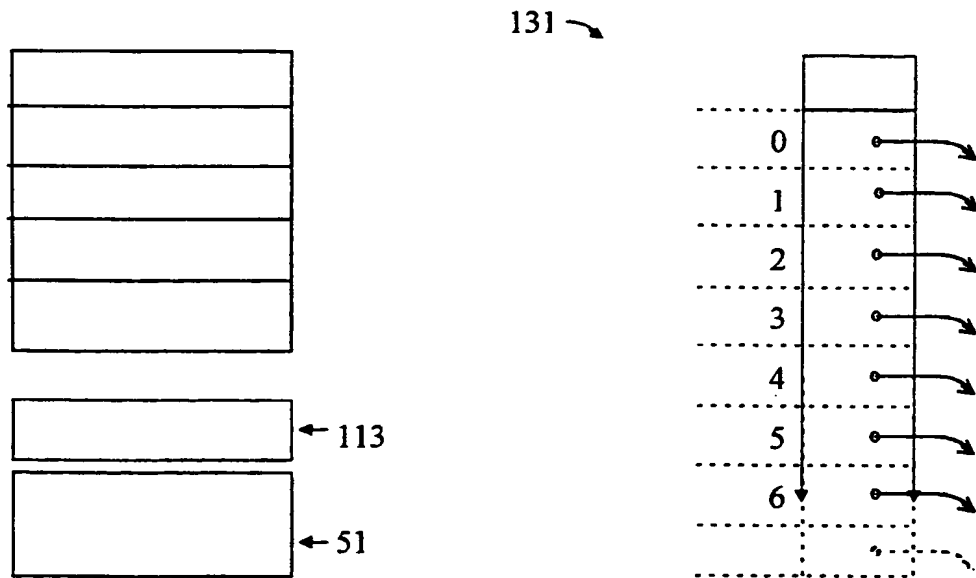

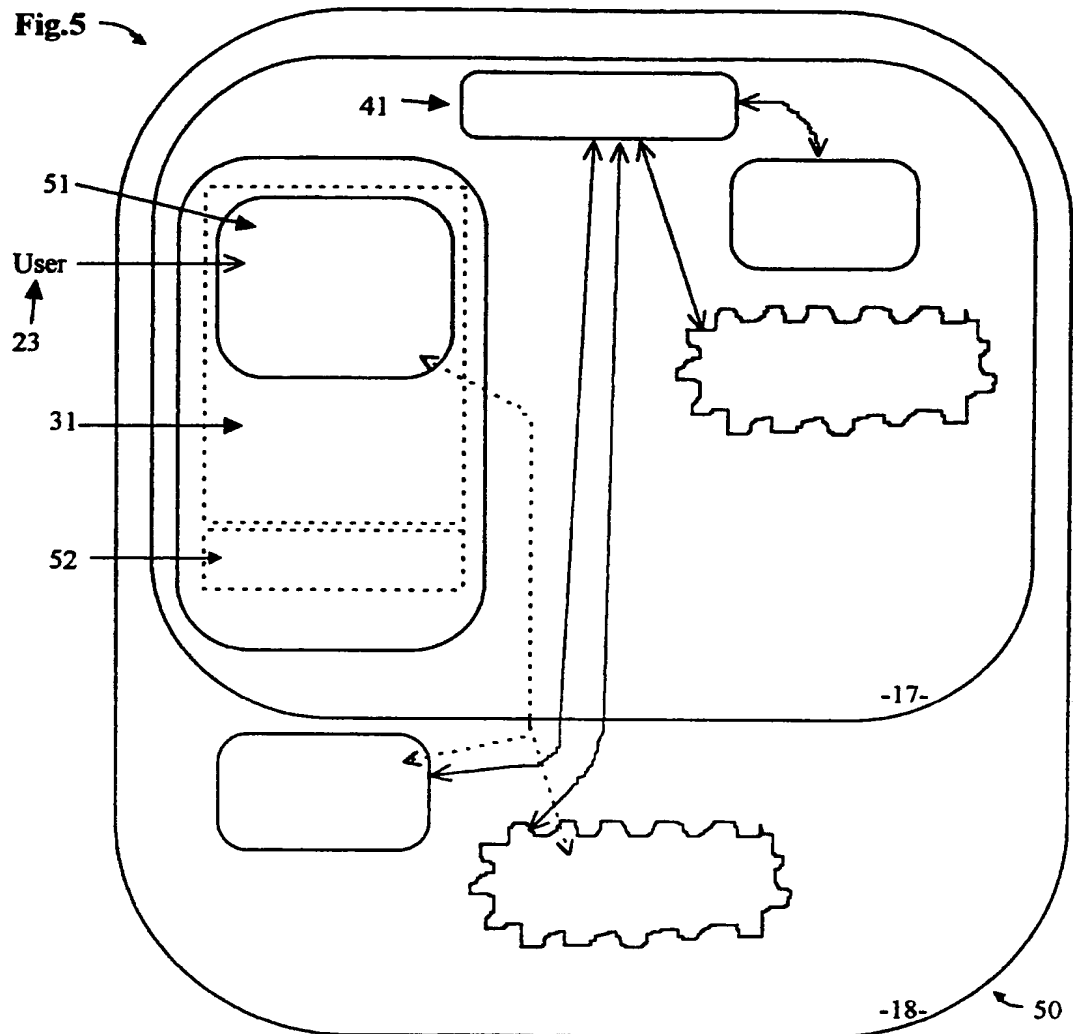


Fig.13



**Fig.5** 



**Fig.6** 

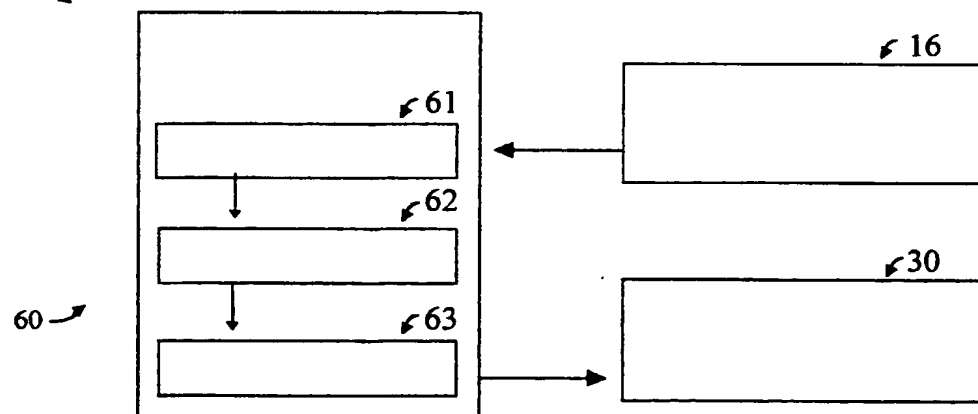


Fig.7

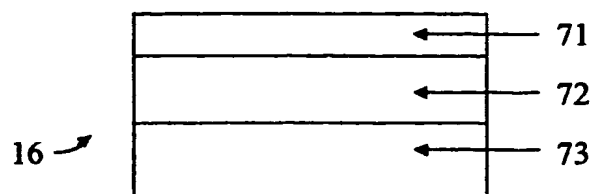
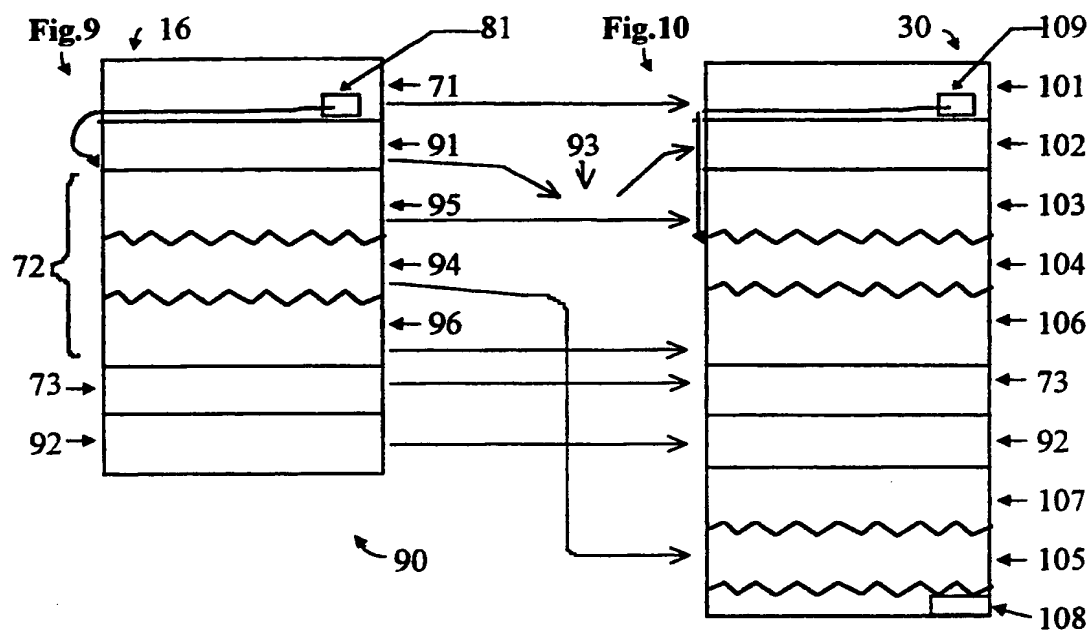
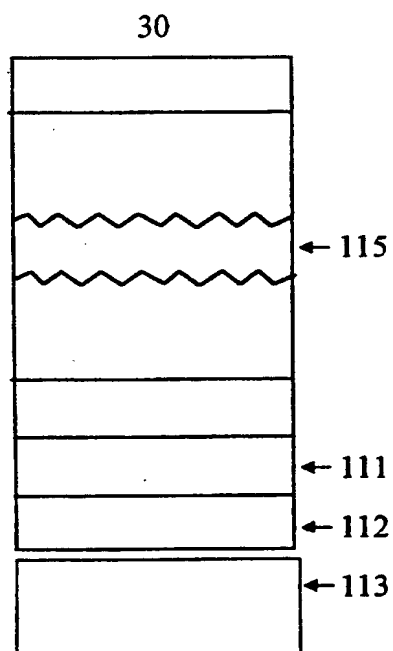
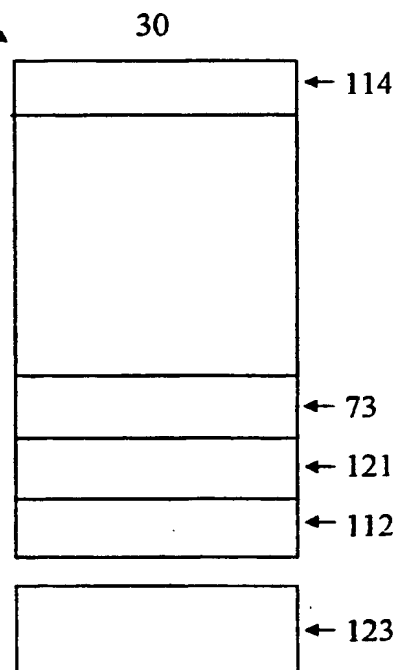


Fig.8

ADDRESS	TYPE
00H	1 word
02H	1 word
04H	1 word
06H	1 word
08H	1 word
0AH	1 word
0CH	1 word
0EH	1 word
10H	1 word
12H	1 word
14H	1 word
16H	1 word
18H	1 word
1AH	1 word
1CH	1 word
xxH	xx
xxH	xx

Diagram illustrating a memory layout table (Fig. 8) and its associated components. The table lists addresses (00H to 1CH, followed by two xxH entries) and their corresponding types (1 word or xx). A vertical arrow on the left indicates a range from 00H to 1CH. A horizontal arrow at the bottom left points to label 71. On the right side, a vertical arrow points to label 82, and a horizontal arrow at the bottom right points to label 81.



**Fig.11****Fig.12**

## INTERNATIONAL SEARCH REPORT

International Application No.  
PCT/AU 96/00440

<b>A. CLASSIFICATION OF SUBJECT MATTER</b>		
Int Cl <sup>6</sup> : G06F 12/14		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b>		
Minimum documentation searched (classification system followed by classification symbols) IPC: as above		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched AU IPC: as above plus G06F 9/445		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) WPAT:INSPEC:PLUS (AUTH:, SECUR:, TAMP:, ACCESS:)		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 568 438 A1 (Gemplus Card Int.) 3 November 1993 whole document	2, 13, 15
X Y	US 4 864 494 (Computerised Data) 5 September 1989 Abstract, col 1-4, Figures	2, 13 35-38, 40-41
X Y	EP 326 700 (IBM) 9 August 1989 whole document	1 5, 6, 8, 11, 48
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C <input checked="" type="checkbox"/> See patent family annex		
<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p>		
Date of the actual completion of the international search 20 September 1996		Date of mailing of the international search report 3 OCT 1996
Name and mailing address of the ISA/AU AUSTRALIAN INDUSTRIAL PROPERTY ORGANISATION PO BOX 200 WODEN ACT 2606 AUSTRALIA Facsimile No.: (06) 285 3929		Authorized officer  DALE SIVER Telephone No.: (06) 283 2196

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 600 184 (VOQT) 18 December 1986 Abstract, Figures	2, 13, 15
Y	"State Transition Analysis: A Rule-Based Intrusion Detection Approach" (Ilgun et al.) From IEEE Transactions on Software Engineering, Vol.21, No.3, March 1995 (pp 181-199), Abstract	1, 8, 42
Y	"To Whom am I speaking" (Lomas et al.) from IEEE Computer, Vol.28, No.1, January 1995 pp 50-54 Whole document	1, 2, 6, 35
Y	WO 92/14209 (Toven Technologies Inc.) 20 August 1992 Whole document	1, 2, 4, 5, 11, 14, 25, 36, 48
Y	WO 88/03287 (Harcom Security Systems) 5 May 1988 Whole document	1, 2, 4, 14, 37, 38, 40, 41

**INTERNATIONAL SEARCH REPORT**

International Application No.  
PCT/AU 96/00440

**Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)**

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

**Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

Claim 1 - secure input routine for ID-Data with anti-spy, anti-tamper.

Claim 2 - altered secure executable program with encryption.

Claim 3 - secure entry with audio/visual display.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.  
☐ No protest accompanied the payment of additional search fees.

# INTERNATIONAL SEARCH REPORT

International Application No.

**PCT/AU 96/00440**

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	9214209	AU	12009/92	CA	2035697	US	5325430
EP	568438	FR	2690540				
EP	326700	DE	3852292	JP	2007640	US	4945468
US	4864494	NONE					
WO	8803287	AU	82321/87				
FR	2600184	NONE					

END OF ANNEX

